

|  |
| --- |
|  |
| Závěrečná zpráva testu bezpečnosti |
| Autor: SecurIT |
| Zákazník: Jméno |
| Datum: 24.07.2019 |  |
|  |

*Obsah tohoto dokumentu je důvěrný a slouží čistě pro potřeby zákazníka. Jakékoliv publikování či kopírování bez vědomí zákazníka je přísně zakázáno.*

**Obsah**

[1. Účel testu 3](#_Toc14871144)

[2. Cíl testu 3](#_Toc14871145)

[3. Zranitelnosti 3](#_Toc14871146)

[4. Shrnutí 4](#_Toc14871147)

[5. Odkazy 4](#_Toc14871148)

# Účel testu

Tento dokument shrnuje nálezy bezpečnostních testů, vykonaných pro zákazníka Jméno.

# Cíl testu

Testy byly provedeny, dle domluvy se zákazníkem, na následující adrese:

* [http://vas\_server.cz/](http://testphp.vulnweb.com/)

*V přílohách jobu jsou přiložené výstupy automatických scannerů z veřejně zranitelného webu, který provozuje společnost Acunetix právě za tímto účelem – demonstrování nalezení zranitelností. Nejedná se o skutečnou produkční zranitelnou stránku.*

Aplikace je dostupná z prostředí intenetu.

Pro zvýšení efektivity testování byly využity automatizované a semi-automatizované nástroje, adaptované skripty a manuální procedury. Jednalo se jak o komerční, tak i volně dostupné nástroje.

# Zranitelnosti

|  |  |  |
| --- | --- | --- |
| Závažnost | Název | Popis |
| 9/10 | **SQL Injection** | Parametr “cat” na stránce [http://vas\_server.cz/listproducts.php](http://testphp.vulnweb.com/listproducts.php) je zranitelný na SQL Injection. Pomocí zranitelnosti se může útočník dostat k celé databázi serveru. |
| 8/10 | **Nešifrované spojení** | Stránka je dostupná pouze na HTTP (ne na HTTPS), útočník může odposlechnout všechny údaje, které uživatel do stránky vloží (včetně hesel).  |
| 8/10 | **XSS – Cross Site Scripting** | Parametr “cat” na stránce http://vas\_server.cz/listproducts.php aParametr “pp” na stránce [http://vas\_server.cz/hpp](http://testphp.vulnweb.com/listproducts.php) a parametr “searchFor” na stránce [http://vas\_server.cz/](http://testphp.vulnweb.com/listproducts.php) je zranitelný na XSS. Pomocí zranitelnosti může útočník ukrást Cookie se Session ID a dostat se tak uživatelům do jejich účtu. |
| 7/10 | **Zastaralá verze PHP** | Na serveru běží zastaralá verze PHP 5.1.6, která obsahuje veřejně známé zranitelnosti. |
| 6/10 | **Detekce phpinfo.php** | Na adrese [http://vas\_server.cz/secured/phpinfo.php](http://testphp.vulnweb.com/secured/phpinfo.php) je volně dostupý soubor phpinfo, který útočníkovi prozrazuje nastavení serveru. |
| 6/10 | **Procházení adresářů** | [http://vas\_server.cz/CVS/](http://testphp.vulnweb.com/CVS/)[http://vas\_server.cz/Templates/](http://testphp.vulnweb.com/Templates/) [http://vas\_server.cz/admin/](http://testphp.vulnweb.com/admin/) [http://vas\_server.cz/images/](http://testphp.vulnweb.com/images/)Adresy uvedené výše je možné volně procházet. Útočník z nich může stáhnout citlivé soubory. |
| 3/10 | **Informace z chybových hlášek** | Podle chybové hlášky při testování SQL Injection může útočník zjistit, že backend databázový server je MySQL. Poté může hledat zranitelnosti přesněji a cílit svoje útoky pouze na tento system. |
| 3/10 | **Informace z hlaviček** | Z hlaviček odpovědí webového serveru může útočník zjistit, že web je provozovaný na serveru nginx verze 1.4.1 a PHP 5.1.6 – podle toho může přesněji cílit své útoky. |
| 2/10 | **Chybí bezpečnostní hlavičky** | Server v odpovědích nezasílá hlavičky:* X-Content-Type-Options
* X-Frame-Options
* X-XSS-Protection

Nepoužívání těchto hlaviček se neslučuje s best practices tvoření webových stránek a v určitých situacích může útočníkovi pomoci v provádění jiných útoků. |
| 1/10 | **Metoda OPTIONS** | Na webovém serveru je povolená metoda OPTIONS. Podle best practice by měly být všechny nepoužívané metody webového serveru zakázány. |

V případě potřeby je možné informace k jednotlivým nálezům dohledat v zaslaných přílohách.

# Shrnutí

**Celkové hodnocení bezpečnosti: 15%**

Na server se nacházejí vážné zranitelnosti, pomocí kterých se útočník může zmocnit databáze, uložených souborů, nebo zjišťovat konfiguraci serveru. Pomocí ostatních zranitelností může přesněji cílit útoky a hledat konkrétní exploity.

# Odkazy

Bezpečnostní metodika OWASP:

* OWASP Project - [https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project](https://www.owasp.org/index.php/Category%3AOWASP_Top_Ten_Project)