



software security



ULESKA

Proactive Software Security

ULESKA PROFESSIONAL SERVICES

TRAINING & CONSULTING

ULESKA LTD

16 MOUNT CHARLES, BELFAST

ULESKA PROFESSIONAL SERVICES

At Uleska we provide professional training and consulting security services to the UK & Irish software industries. Uleska's personnel are highly skilled in software development and application security disciplines, combining decades of professional software development experience with certifications and thought leadership in cyber-security.

All Uleska consultants hold industry recognized cyber-security certifications such as CISSP (Certified Information Systems Security Professional), CSSLP (Certified Secure Software Lifecycle Professional) or CEH (Certified Ethical Hacker), as well as having hands on experience of developing software.

Uleska professional services include the following training and consulting services. Click through for more details, or contact us for more information.

CUSTOM-BUILT SOFTWARE SECURITY COURSES

Software companies often wish to focus training on specific security aspects or issues, and at Uleska we made to measure software security training to teams in many industries. These courses can cover secure coding, penetration testing, secure SDLC, devsecops, and other aspects of software security.

ESTABLISHED SOFTWARE SECURITY COURSES

Established training courses teaching the latest proven techniques in secure software development and security testing. These include courses aimed at software developers, and software testers, as well as teaching threat modeling techniques to ensure security is considered at the architecture and design stage of a project.

PENETRATION TESTING

Ensuring an application is secure against attackers and threats is a must for modern software. With our experience of end-to-end and web security at some of the world's largest banks, we understand the need to protect against each and every vulnerability.

SECURITY ENGINEERING

Uleska has extensive experience designing and implementing security features into projects across several industries. We can join your existing development teams to perform secure coding, implement web security features, threat model application architecture and designs, and incorporate devsecops into your organization.

SECURE CODE REVIEWS

Uleska has extensive experience of secure coding and conducting secure code reviews, either at the end of a project, or proactively as part of the software development lifecycle (SDLC).

SECURE SDLC (SOFTWARE DEVELOPMENT LIFECYCLE)

Our team of software security experts and security testers can assist your company in creating an environment where security is a natural part of a development project, not just an afterthought.

TRAINING SERVICES

At Uleska we can help you understand your software security challenges, and prepare you to overcome them. With extensive industry and software security experience we can provide relevant, targeted training courses for your teams.

Uleska provides both bespoke and established software security training courses to suit the needs of any company. All training is delivered by professionals experienced in software security, including security architects and persons representing the OWASP and ISC² organizations.

CUSTOM-BUILT SOFTWARE SECURITY COURSES

Software companies often wish to focus training on specific software or web security issues. At Uleska we have extensive experience of providing this type of specific software security training to teams in many industries. We can work with you to combine training elements to develop a course geared towards your needs, or develop new training elements specific to your product or industry.



Whether it be follow-up training to focus on issues discovered during security testing, or targeted training on new technologies such as cloud or IoT, Uleska can bring together the necessary package for you and deliver it to your software teams. We also measure the impact of the training course to ensure its effectiveness. These courses can cover secure coding, penetration testing, secure SDLC, devsecops, and other aspects of software security

Speak to Uleska to discuss your specific security needs and we can work with you to put together a training package that empowers your teams to be effective and secure.

Duration	Delivery Options	Cost
Depends on scope, typically between 1 – 5 days.	Can be delivered as classroom training, or online	Depends on scope. Contact Uleska for a quote.

ESTABLISHED SOFTWARE SECURITY COURSES

SOFTWARE SECURITY TRAINING FOR DEVELOPMENT TEAMS

This two-day course is geared towards software developers, enabling them to understand the most common technical software issues in today's industry. This course covers the OWASP Top 10 plus the SANS Top 25, providing real life examples of breaches and countermeasures.

This course is suitable to beginner and intermediate levels, and includes both theory and hands-on experience of exploitable code, explaining how an attacker can find a software vulnerability, and exploit it.



SOFTWARE SECURITY TRAINING FOR TESTING TEAMS



This two-day course is geared towards quality assurance teams, empowering them to discover and security test common issues in developing software. This course covers industry standard lists such as the OWASP Top 10 and the SANS Top 25 issue lists, describing the nature of the attacks and testing any software application to determine if the vulnerability exists.

This course is suitable to beginner and intermediate levels, including both theory and hands-on experience of exploitable code. Participants will be able to introduce security testing into the secure SDLC.

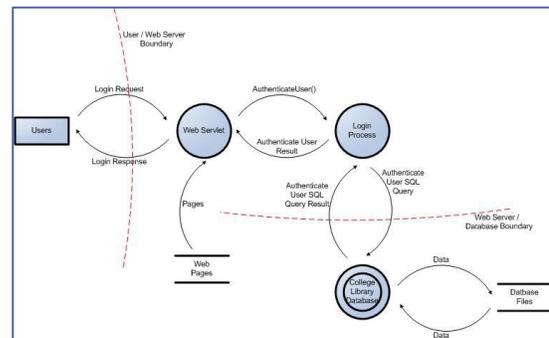
INTRODUCTION TO THREAT MODELING

In today's application security industry, many companies understand that product architecture and design flaws can have a major impact. Applications can be bug free, however design flaws can still expose sensitive data, or cause other non-compliances with industry regulations.

Threat Modeling is the systematic, methodical process used by security experts to determine if a product's architecture and design are vulnerable to attackers.

This two-day training course introduces the attendee to the Threat Modeling process. We conduct a Threat Modeling exercise on an example application, covering the theory as well as practice. At the end of the course the attendee will be able to conduct a Threat Model on any web or backend application.

Threat Modeling aspects covered include: high level security objectives, attack surface determination, asset evaluation, entry point detection, threat agents, data flow diagrams, threat enumeration, security requirements, use/abuse cases.



Training Duration	Training Delivery	Training Cost (exc. VAT)
All courses are 2 days in length.	Can be delivered as classroom training, or online.	£395/person for public class, or £2,000/course for in-house delivery

CONSULTING SERVICES

At Uleska we have extensive experience not only in application security, but also in the modern day practice of software development. This means the services we provide will not only secure your current software suite, but also empower your software teams with actions to maintain that security throughout the entire software development lifecycle.

PENETRATION TESTING

Ensuring an application is secure against attackers and threats is a must for modern software. With our experience of end-to-end and web security at some of the world's largest banks, we understand the need to protect against each and every vulnerability. This is why we combine cutting edge automated security tools with years of software security experience to ensure your software is secure from threats of all kinds.



While your software is security tested, we will provide updates if major issues are found, allowing you to take action immediately. Our focus on proactive software security means we work to ensure you not only know what issues exist, but also how to fix them through configuration or code changes.

We can also point to industry resources, or provide follow-up training, based specifically on the types of security issues experienced by your software.

SECURITY ENGINEERING



Uleska has extensive experience designing and implementing security features into projects across several industries. We can join your existing development teams to implement security features, threat model application architecture and designs, and incorporate security into your organization.

From encrypting application data at rest or in transit, to effective input valuation and component authorization, Uleska has coded many security features in development languages such as Java, C#, C++ and Python. We can integrate with existing development teams to take on security stories, ensuring security regulations and standards are met within the product codeline.

SECURE CODE REVIEWS

```

resource_id = $role_details['id'],
resource_id = $resource_details['id'],
);
if ( $this->rule_exists( $resource_details['id'], $role_details['id'] ) ) {
    if ( $success == false ) {
        // Remove the rule as there is currently no need for it
        $this->sql->delete( 'acl_rules', $details );
    } else {
        // Update the rule with the new access value
        $this->sql->update( 'acl_rules', array( 'access' => $access ) );
    }
}
foreach( $this->rules as $key=>$rule ) {
    if ( $details['role_id'] == $rule['role_id'] && $details['resource_id'] == $rule['resource_id'] ) {
        if ( $success == false ) {
            unset( $this->rules[ $key ] );
        } else {
            $this->rules[ $key ]['access'] = $access;
        }
    }
}

```

Industry sources¹ cite secure code reviews as one of the most effective methods for finding some types of software security issues, such as privacy, business logic, direct object references and security misconfigurations. Experience also shows us that particular modules or code areas produce higher numbers of security issues than others, either due to coding issues or the sensitive nature of the module.

Uleska has extensive experience in conducting secure code reviews, either at the end of a project, or as part of the software development lifecycle.

SECURE DESIGN AND THREAT MODELING

Proactively addressing security during the architecture and design of software can reduce the overall security costs in a project. When a design decision causes a security issue, then the redesign and recoding necessary to fix the vulnerability can hold up releases and engineers.

At Uleska we can examine the design and architecture of your project or application, and provide a threat modeling service which ensures security is covered. Threat modeling identifies the assets your software needs to protect, the entry points and trust boundaries where those assets are available, and the threat actors who would benefit from stealing those assets. We can then identify any flaws in the current design which exposes those assets to threat actors and recommend changes to protect the application from compromise.



¹ See OWASP Code Review Guide v2 https://www.owasp.org/index.php/File:OWASP_Code_Review_Guide_v2.pdf

SECURE SDLC (SOFTWARE DEVELOPMENT LIFECYCLE)



Our team of software security experts can assist your company to create an environment where security is a natural part of a development project, not just an afterthought. Multiple trials and experiments show that incorporating security practices into project planning, design and implementation can reduce costs and improve development timelines.

We provide consultancy and advice to customers who wish to:

- Discover new ways to incorporate software security procedures into their SDLC.
- Comply with relevant industry regulations such as PCI DSS, HIPAA, GDPR and others.
- Scale their software security practices to meet customer demand.
- Apply software security practices to today's development methodologies including Agile and DevOps.

Consulting Duration	Consulting Delivery	Consulting Cost (exc. VAT)
Depends on scope, typically 2-5 days.	All consulting delivered onsite, in collaboration with your software teams.	£400/day

CONTACT ULESKA

To find out more about Uleska Professional Services, and obtain a quote, contact us through our website at www.uleska.com, or email info@uleska.com.